1. Context

"It's personal. It's private. And it's no one's business but yours." This is how Phil Zimmermann, the author of the popular PGP program[1], summarizes the many reasons why we should encrypt data. Now that a good proportion of the population is connected via the Internet, this statement is truer than ever.

The original Internet protocols (also referred as the TCP/IP protocols) have not been designed with security as the top priority. Most of the data sent over the Internet is thus sent as "clear text" and anyone has the potential to eavesdrop on your e-mail or on your connection to a specific server, trying to steal your password and take control of your account.

Every e-mail that you send and receive is traveling through the whole planet in a clear-text format. Thus, it is the equivalent of writing to anyone using a post card and sending it via the standard mail: no more privacy. Although your vacation memories might not be the most sought after information, any kind of information pertaining to the nature of your business is very precious and could jeopardize the integrity of the whole corporate structure.

Prior to deciding whether to encrypt data or not, it is essential that an adequate data classification exists. Such an examination of our data establishes the sensitivity of data and the threats that face it.

2. Guidelines

2.1. Encryption solutions

Encryption is a serious activity that needs to be undertaken with a serious framework in place. No one should, on their own, decide to go one direction, but it must be planned at the corporate level in order to ensure consistency and manageability. Still, solutions abound for general as well as specific needs.

Encryption may take many forms, from a simple character permutation to elaborate algorithms involving large prime numbers and keys of different sizes. It is important to

[1] See the Web document entitled "Why do you need PGP?" by Phil Zimmermann at http://www.pgpi.org/doc/whypgp/en/

choose the appropriate encryption method and many factors will influence one's decision:

- corporate standard;
- sensitivity level of the information;
- perceived threat and associated risk level.

No one method is THE ultimate method and encryption methods have both their strength and some drawbacks.

2.1.1. Zip compression

A well-known utility in use on most workstations today, the Zip archive format supports the industry standard Zip 2.0 encryption format. It is a weak measure against content theft, but it will give a reasonable protection against casual users. Furthermore, a set of files can be grouped together and protected by a unique password which reduces greatly the number of individual passwords that are required within your environment.

As the help file from WinZip 8.0 states, "Password protecting files in a Zip file provides a measure of protection against casual users who don't have the password and are trying to determine the contents of your files. The Zip 2.0 encryption format, however, is not as secure as DES and the RSA public key formats used by programs such as PGP, and does not provide absolute protection against determined individuals with advanced cryptographic tools."

When choosing a password to protect your Zip, remember to use caution and apply the principles described in the internal document entitled "Guidelines for Secure Password Selection". One must also keep in mind that there is no "back door" to open such a file if the password is lost: you must redo the work included in the protected file.

2.1.2. « Application specific » encryption

Many workstation applications such as the Microsoft Office suite offers function to "password protect" your documents, effectively encrypting your document. Although still considered a weak encryption scheme, password protected files will deter the casual user from seeing and/or modifying files considered sensitive enough to protect in this matter.

2.1.3. DES, RSA and other encryption algorithm

Cryptographers have been hard at work for the last 50 years, creating devices and algorithms to encrypt data. Most of these algorithms involve the use of a "secret" information (the key) in order to get the operation done and undone. Therefore the communication of this secret information (as for the password, in less robust encryption techniques) is the cornerstone of these technologies. If both parties use different secrets, we say they are using an asymmetric algorithm, whereas if they use the same secret, they use symmetric key algorithms. The latter perform generally much faster than its counterpart, but require a shared secret to be communicated.

Algorithms based on these techniques are hard to break and their strength can generally be increased by the use of longer encryption keys (from 40 to 56 bits, or 128 bits for example) that will diminish the likelihood of someone breaking into your file to almost nothing.

The popular PGP program[2] uses this type of algorithms to encrypt your files. Another strength of PGP is that it can be scaled up to accommodate a whole community of users who wish to exchange information. This requires a systematic management of users and their respective encryption keys[3] in order to establish the trust level of every user's keys through the issuance of a certificate.

2.2. The personal workstation

At the hardware level, many threats justify the use of encryption. The theft of corporate information for unauthorized purposes is an activity that occurs on a regular basis. A CEO might carry the latest business plan on his laptop or PDA and a Marketing VP may have a copy of the latest sales forecast.

Data medium increases in density at a gigantic pace. Nowadays, a 60 Gb hard drive fits in one's pocket and can likely be removed from the host computer in seconds. It is no longer only a matter of computer theft, since data theft can reap bigger benefits. We must protect all of our data with the utmost dedication to avoid information leakage and corporate exposure.

There are many encryption methods available today and they range from compressing the files and protecting the archive with a password (WinZip, for example), to the more robust methods of encryption, such as the use of known algorithm (DES, Triple-DES, RSA, etc).

2.2.1. Desktop computer

Since a desktop computer is, by definition, less likely to be carried, the threats that face it are proportionally smaller: theft of the whole computer, theft of its information media (hard disk, CD-ROM, DVD-ROM, floppy disks and the plethora of external media on the

[2] PGP can be found at www.pgp.com
[3] This kind of infrastructure is referred to as a Public Key Infrastructure or PKI

market) and physical damage (vandalism). One must finally envision data theft through the network connection (sniffing and pulling of data).

Encryption of sensitive information on a file-by-file or folder-by-folder basis is thus an excellent counter-measure to the identified threats (although only a backup will prevent data loss from physical damage), no matter the medium used.

All media must be stored in a locked location and, whenever possible, a locking system must prevent an authorized access to the computer's components on the inside, in order to avoid possible hard disk theft.

2.2.2. Mobile platform

Mobile computers and the growing mobile computing platform (PDA, 2-way pagers and cellular phones) are an easy target for thieves. As such, the potential for data loss and theft is considerably higher that for a desktop computer since laptop are likely to be found outside of the corporate environment, thus rendering corporate physical controls inapplicable. Therefore, the desktop computer guidelines must be considered the foundation on which to build extra measures for this specific platform.

2.2.2.1. Laptop

The hard disk should be encrypted and a startup password should be used to unlock it. The scheme used must allow for access controls even if the hard disk is taken out of the computer as to protect the data in the event of hard disk theft. The encryption algorithm used shall be publicly available (no proprietary algorithm) unless sufficient evidence could support the quality of the proprietary mechanism.

Moreover, an inactivity timer shall be used in order to lock the hard disk after a pre-determined period and a mechanism should allow the user to lock the hard disk at any time.

Data copied to external media for personal archive should be encrypted and proper labeling must be applied to the media for its content, but also for the encryption key owner. The latter will define who can access this media.

2.2.2.2. PDA

Personal Diary Assistants, or PDAs, present a new challenge for information security. As their storage and processor capacity grow, more and more applications, and thus data, can be executed and stored on them.

In this context, dedicated PDAs devices such as the ***PalmPilot***™, ***Windows CE*** compatible equipments or any other model, require some form of encryption for any sensitive data stored on them. Proper care must be taken to insure the identification of such data and its proper removal from the PDA, or transfer to an encryption capable application for safe storage. We must keep in mind, though, that the first and best line of defense to deter the casual onlooker is always the power-on or inactivity password.

Synchronization between these devices and a computer must occur only through a direct connection unless this data transfer can be encrypted with a good level of safety. Proper care must be taken to ensure that data deleted from the PDA for safety purposes is not copied back during the synchronization process.

2.2.2.3. Cellular phone and two-way pagers

Cellular phones and two-way pagers now offer a mix of PDA functions and device specific functions. PDA functions for these devices must be considered to comply with the PDA guidelines (see section 2.2.2.2) while their other functions must be considered separately.

Device specific functions such as e-mail reception and storage, to name a few, must also be reasonably protected from unauthorized eavesdropping and from illegal use (or resell). The first and best line of defense to deter the casual onlooker is always the power-on or inactivity password.

Encryption programs such as PGP are now starting to address this issue and any such utility must be considered, especially if corporate data resides on a device of this category, in any form.

Industry standard protocols[4] will be preferred over proprietary standards, whenever available, to maintain compatibility with other platforms at all times.

2.3. Shared storage

Data is almost always stored on some form of medium at any given time during a computer process: internal hard disk, external disks and arrays, diskette, CD-ROM, DVD-ROM or other types. Information can be stored in user managed files (such as word processing or text documents in an operating system file structure) or it can be stored within a “computer managed structure”, such as binary or text files or an organized database management system (DBMS). Other activities also require data to be stored. Data may reside on a local medium or a remote medium, within a LAN, a WAN or the Internet.

[4] For example, consult the WAP standards at www.wapforum.org

Despite this over simplified view of data storage, the problem of eavesdropping and data theft always surfaces on: one's local data store may be another's external data store and vice-versa. Therefore, one must protect its data by exercising due-diligence regarding the threat level that prevails within the perceived environment.

2.3.1. Internal servers

An internal server is part of a corporate environment either on a LAN, WAN or by using VPN connections. It is protected by appropriately configured firewall equipments and is intended for the sole use of authenticated corporate users. Such servers can be used for user data storage and backup or internal application data.

Although the operating system may provide adequate permission management at the file level, sensitive information should be encrypted according to its sensitivity in order to stop inappropriate modification or unauthorized viewing of the data.

Care must be taken to protect personal data about individuals (such as health record in a Human Resource system or server) and caution must be exercised when handling such data. For example, unencrypted data must never be stored on backup media even though the application that created it uses a strong authentication mechanism. Moreover, the problem could be amplified should these tapes be stored outside of the corporate environment.

Particular attention must be given to database servers located in the LAN/WAN environment. Proper authentication must be enforced and all sensitive information must be encrypted do deter unauthorized use of any information found. Therefore, the use of flat-file text databases must be avoided, unless files can be encrypted with a strong algorithm.

2.3.2. External

Servers located outside the corporate environment are considered “external” to the organization. They include outsourced e-mail servers and file backup servers, amongst others.

These servers are subject to a variety of threats, mainly successive break-in attempts, data modification, data theft, eavesdropping for specific information and data deletion. Threats come from uncontrolled external sources who try to take control of systems that are not hosted and managed by our own resources, following our own defined policies. Therefore, the threat level must be considered high.

Communication with these servers must be secured (see Section entitled *Hosted services*) and the contents should be encrypted, whenever possible, using strong algorithms. No private data should reside on external server unless strong encryption is being used, and this type of information must be kept to an absolute minimum.

2.4. Network traffic

Network traffic can be examined with sniffing equipments. Most TCP/IP protocols carry unencrypted information such as user name and password. Thus a sniffer can grab and see all of this information as long as it can be installed on the appropriate network segment inside the network.

Sniffers can be legitimate corporate tools that are used for monitoring of the network, but they can also be used maliciously by unauthorized users who wish to gather more information than they are authorized to. In all cases, this type of tools shows private information such as user name and password, but also message and file contents (where SMTP or FTP, for example, are being used). User names and password must be encrypted to maintain user accountability and non-repudiation.

Therefore, proper evaluation is crucial to determine if network traffic encryption is required. Corporate security policy must outline the requirements for such an activity and its extent.

2.5. Access to networking equipment

Remote access to networking equipment must be made through an encrypted session, such as SSH. Encryption keys must be negotiated as to insure proper authentication, and password based authentication must be avoided where possible.

2.6. Hosted services

Services hosted by a third party, outside of the corporate environment present a dual challenge: on one hand they store corporate information on a platform that is outside of our control (see section 2.3.2 in this document) and on the other hand, we must exchange information with this outside environment in an all secure way.

The preferred method of communication between the corporate environment and any outside partner must insure that this communication may not be intercepted and deciphered. Encryption is therefore required when accessing a hosted service. For example, Secure Socket Layer version 3 (SSL3) could be used for this purpose

2.7. The mail exchange

Transfer of information in an unencrypted way does present a threat (see section 2.4 for more information). The protocol we use to exchange e-mail exhibits this behavior with little that can be done without loosing compatibility between systems.

The SMTP protocol is, as its name implies, a very simple protocol and encryption has never been designed into it[5]. Therefore, special measure must be put in place for the protection of the e-mail exchange.

Every e-mail exchanged with the SMTP protocol should therefore be encrypted in order to insure privacy of the communication. Encryption should be strong.

2.8. Other issues

None.

❖ ❖ ❖ ❖ ❖ ❖ ❖

[5] S/MIME and PGP address this issue but are part of not part of the SMTP specification.